FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1389544-0

Total Deleted Page(s) = 68
Page 3 ~ b3; b6; b7C; b7E;
Page 4 ~ b3; b6; b7C; b7E;
Page 5 ~ b3; b6; b7C; b7E;
Page 7 ~ b3; b6; b7C; b7E;
Page 8 ~ b3; b6; b7C; b7E;
Page 9 ~ b3; b6; b7C; b7E;
Page 10 ~ b3; b6; b7C; b7E;
Page 11 ~ b3; b6; b7C; b7E;
Page 12 ~ b3; b6; b7C; b7E;
Page 13 ~ b3; b6; b7C; b7E;
Page 14 ~ b3; b6; b7C; b7E;
Page 15 ~ b3; b6; b7C; b7E;
Page 16 ~ b3; b6; b7C; b7E;
Page 17 ~ b3; b6; b7C; b7E;
Page 18 ~ b3; b6; b7C; b7E;
Page 19 ~ b3; b6; b7C; b7E;
Page 46 ~ Duplicate;
Page 52 ~ b7E;
Page 53 ~ b7E;
Page 54 ~ b7E;
Page 55 ~ b7E;
Page 56 ~ b7E;
Page 57 ~ b7E;
Page 58 ~ b7E;
Page 59 ~ b7E;
Page 108 ~ b6; b7C; b7E;
Page 109 ~ b6; b7C; b7E;
Page 110 ~ b6; b7C; b7E;
Page 111 ~ b6; b7C; b7E;
Page 112 ~ b6; b7C; b7E;
Page 113 ~ b6; b7C; b7E;
Page 114 ~ b6; b7C; b7E;
Page 115 ~ b6; b7C; b7E;
Page 116 ~ b6; b7C; b7E;
Page 117 ~ b6; b7C; b7E;
Page 118 ~ b6; b7C; b7E;
Page 119 ~ b6; b7C; b7E;
Page 120 ~ b6; b7C; b7E;
Page 121 ~ b6; b7C; b7E;
Page 122 ~ b6; b7C; b7E;
Page 123 ~ b6; b7C; b7E;
Page 124 ~ b6; b7C; b7E;
Page 125 ~ b6; b7C; b7E;
Page 126 ~ b6; b7C; b7E;
Page 127 ~ b6; b7C; b7E;
Page 128 ~ b6; b7C; b7E;
Page 129 ~ b6; b7C; b7E;
Page 130 ~ b6; b7C; b7E;

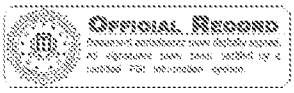
Page 131 ~ b6; b7C; b7E;
Page 132 ~ b7E;
Page 133 ~ b7E;
Page 134 ~ b7E;
Page 135 ~ b7E;
Page 136 ~ b7E;
Page 137 ~ b7E;
Page 138 ~ b7E;
Page 139 ~ b7E;
Page 141 ~ b7E;
Page 142 ~ b7E;
Page 143 ~ b7E;
Page 144 ~ b7E;
Page 148 ~ b7E;
Page 156 ~ b7E;
Page 157 ~ b7E;
Page 158 ~ b6; b7C; b7E;
Page 161 ~ b7E;
Page 167 ~ b6; b7C; b7E;
Page 180 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

[redacted]

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED



FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) To request case be opened **Date:** 03/06/2017

CC: [redacted]

From: ATLANTA
AT-CY1
Contact: SA [redacted]

b3
b6
b7C
b7E

Approved By: SSA [redacted]

Drafted By: SA [redacted]

Case ID #: [redacted] (U) UNSUB(S);
KENNESAW STATE UNIVERSITY - VICTIM;
COMPUTER INTRUSION - CRIMINAL MATTER;

Synopsis: (U) To request case be opened and assigned to the writer.

[redacted] set to expire

Details:

On March 1, 2017, a professor at Kennesaw State University ("KSU") was contacted by an Atlanta-based security firm about an alleged vulnerability in the KSU website elections.kennesaw.edu that contains voter registration information for counties across the state of Georgia. The Atlanta-based security firm was contacted by a security researcher that found the vulnerability and was able to exploit the vulnerability. This allowed the security researcher to obtain the voter registration information. The professor immediately notified KSU's Chief Information Security Officer ("CISO") about the potential vulnerability.

b7E

KSU notified the FBI about the incident. On March 3, 2017, the FBI met with members of the KSU to discuss the incident.

Based on the above information, the writer requests a [redacted]

UNCLASSIFIED

[redacted]

b3
b7E

Title: (U) To request case be opened
Re: [redacted] 03/06/2017

[redacted] and assigned to the writer.

♦♦

FD-941 (2-26-01)

CONSENT TO SEARCH COMPUTER(S)

I, Stephen C. Gay, have been asked by Special Agents of the Federal Bureau of Investigation (FBI) to permit a complete search by the FBI or its designees of any and all computers, any electronic and/or optical data storage and/or retrieval system or medium, and any related computer peripherals, described below:

Dell, PowerEdge R610, Service Tag: 96J2FQ1
CPU Make, Model & Serial Number (if available)

Storage or Retrieval Media, Computer Peripherals

and located at CES, 1000 Chastain Rd Kennesaw GA, which I own, possess, control, and/or have access to, for any evidence of a crime or other violation of the law. The required passwords, logins, and/or specific directions for computer entry are as follows: _____.

I have been advised of my right to refuse to consent to this search, and I give permission for this search, freely and voluntarily, and not as the result of threats or promises of any kind.

I authorize those Agents to take any evidence discovered during this search, together with the medium in/on which it is stored, and any associated data, hardware, software and computer peripherals.

3-3-17
Date

x [signature] C. G

3-3-17
Date

[redacted]
Printed Full Name of Witness

b3
b6
b7C
b7E

Location

[redacted]

MF 3/7/17

b3
b7E

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 03/10/2017

[redacted] date of birth (DOB) [redacted], was interviewed at his residence located at [redacted] After being advised of the identity of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

[redacted] is a [redacted] at a company named BASTILLE located at 1000 Marietta Street, Suite 224, Atlanta, Georgia. The company specializes in research on enterprise threats through software-defined radio. Prior to working for BASTILLE, [redacted] worked for the Oak Ridge National Lab (ORNL) located in Oak Ridge, Tennessee. [redacted] stated he left ORNL to explore working at a start-up company.

In the summer of 2016, [redacted] stated he wanted to research election voter machines and whether they were susceptible to various wireless vulnerabilities among other attacks. [redacted] initially reached out to the Fulton County Government Center in order to obtain an election voter machine. However, personnel at the Fulton County Government Center instructed [redacted] to contact Kennesaw State University (KSU) since KSU oversees Georgia's election operations and voting machines.

b6
b7C
b7E

Prior to contacting KSU, [redacted] conducted research on KSU's Center for Election Systems (CES) website (elections.kennesaw.edu). [redacted] stated he used a technique known as [redacted] In using this technique against the CES website, [redacted]

In addition, [redacted] identified that the CES website was running a [redacted]. Lastly, [redacted] research showed KSU's CES was utilizing the [redacted]

Investigation on 03/03/2017 at Atlanta, Georgia, United States (In Person)

File # [redacted] Date drafted 03/07/2017

by SA [redacted]

b3
b6
b7C
b7E

contacted Merle King who is the Executive Director at KSU's CES about his findings and his interest in conducting vulnerability research on the election voting machines. King stated KSU would "look into" his findings. However, King was not very receptive of the idea of researching the election voting machines. In fact, King told that the people downtown would not appreciate him poking around and "just needed to drop it." stated during this time he consulted with the Electronic Frontier Foundation (EFF) to make sure that he was not violating any laws. advised he maintained all of his communications with King and KSU should the FBI need them.

was unsuccessful in finding alternative contacts at KSU to discuss this matter so he just dropped it. stated he thought about contacting the FBI but did not want to get things spun up prior to the elections.

recalled, on or about Wednesday, March 1, 2017, he was having drinks with who described as being in the security research community. During this time, and started discussing the 2016 elections. told about his initial findings related to the CES website and King's response. told that he knows who is a professor at KSU who could help if the website was still vulnerable. stated he would check and let know.

On the same day, stated he ran This data included Georgia's voter registration records. reviewed some of the data which included training material on how to setup an election voting machine.

b6
b7C
b7E

stated he ran did not know the specific IP address that was assigned to him at the time he executed the script. However, stated he uses the Internet Service Provider Gigamonster.

At the time of the interview, still had a copy of the data downloaded from the CES website but had not disseminated the data to anyone. Special Agent instructed to delete the data which agreed to do.

At the conclusion of the interview, expressed concern about the state of the CES website and asked the agents if anything was going to be done about it being wide-open. stated, if he had malicious intent,

b3
b6
b7C
b7E

[redacted] stated he could be contacted via his cell phone number [redacted]

[redacted]

3/3/17

- Aug 16 -

[redacted]

b6
b7C
b7E

[redacted]

last Wed - Friday

Server appeared to have been [redacted] vuln since 2013 -

- Giga monster - ISP

-

[redacted]

spoke w/ ACLU - EFF

b3
b7E

FD-302 (Rev. 5-8-10)

UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION

Date of entry 03/10/2017

On March 3, 2017, representatives from the Atlanta Division of the Federal Bureau of Investigation (FBI) as well as the United States Attorney's Office, Northern District of Georgia (USAO-NDGA), met with executives of Kennesaw State University (KSU). The individuals in attendance included:

Federal Bureau of Investigation
[redacted] Supervisory Special Agent
[redacted] Special Agent
[redacted] Special Agent
[redacted] Computer Scientist

United States Attorney's Office
[redacted] Assistant United States Attorney

Kennesaw State University
Lectra Lawhorne, Chief Information Officer/VPIT
Stephen C. Gay, Chief Information Security Officer
Jeff Milsteen, Chief Legal Affairs Officer
Andrew Newton, Associate General Counsel

b6
b7C
b7E

KSU Executives provided the FBI with a document outlining the event up to March 1, 2017. In summary, GAY was contacted by [redacted] a professor in the Information Assurance and Security Program regarding a third party report he had received from an "Atlanta based security firm" which alleged users were able to exploit KSU's Center for Election Systems (CES) website (elections.kennesaw.edu) [redacted] counties across the State of Georgia. Following this notification, GAY initiated KSU's [redacted]

GAY's team did not obtain a volatile memory dump or a forensic image of the server hosting the CES website. The server was powered off and placed in a secure room. GAY stated his team is maintaining a Chain of Custody for the server.

GAY advised the files that were accessible contained voter data to

Investigation on 03/03/2017 at Kennesaw, Georgia, United States (In Person)

File # [redacted] Date drafted 03/07/2017

by [redacted] SA [redacted]

b3
b6
b7C
b7E

include: ~~Name, Address, Last four digits of SSN,~~ DOB, ~~Driver's License~~ Number, and Party Affiliation. He also stated some of the records may contain full SSNs as the State of Georgia previously used SSNs as an individual's Georgia Driver's License Number.

GAY stated KSU was able to preserve log files from the server to include both the [redacted] b7E

[redacted]

GAY stated in August 2016, a security researcher from BASTILLE in Atlanta, Georgia had contacted KSU regarding a vulnerability associated with CES website and KSU had addressed it.

GAY identified MERLE KING as the Executive Director of the Center for Election Systems. KING would be able to answer any questions about who should have legitimate access to the CES website.

A digital copy of the summary provided by GAY has been placed in the 1A section of the captioned case file.

Center for Elections System Incident – 03/01/2017

Incident background:

Stephen Gay (KSU CISO) was contacted by Professor [redacted] (KSU [redacted] Professor) regarding a 3rd-party report he had received from an "Atlanta based security firm". This initial call was at 9:29pm on Wednesday March 1st and alleged that through the use of [redacted] for counties across the State of Georgia. Stephen immediately activated the UITS incident response team to validate the vulnerability, which was confirmed by the senior engineer. Stephen notified Lectra Lawhorne (KSU CIO), at 11:00pm regarding the notice and vulnerability. At 11:20pm, [redacted]

b6
b7C
b7E

Potential Impact:

High. The discovered vulnerability is challenging to recreate, requiring [redacted]

b7E

Current progress:

Members of the UITS Information Security Office [redacted] met with members of the Center for Election Systems (Merle King, [redacted] and Michael Barnes) on 03/02/17 to discuss the incident, extract the logs for analysis, and begin aligning resources toward the hardening of the elections.kennesaw.edu servers. The Center Director, Mr. King, informed all parties that he would need to keep the Georgia Secretary of State "in the loop" since he (The Secretary of State) was the data custodian for the Center of Elections data. Mr. King further advised that he had been in contact with him regarding the incident and that the Secretary of State was "ok" with our investigation although he requested to receive regular updates.

b6
b7C
b7E

Stephen Gay briefed the CIO regarding the incident and notified the USG HelpDesk regarding this incident, per KSU Incident Response Procedures (USG Ticket number USG-INC0014152). At 11:00am on 3/2/17, UITS began [redacted] elections.kennesaw.edu [redacted] extend back to February 16th, 2017 due to system configuration and initial examination identified a single database file which contained 6.7 million records of what appears to the voter data. At 3:24pm, log review determined that:

- 40 IP Addresses accessed 1 or more database files
- 17 IP Addresses accessed 1 or more zip archives

At 4:30pm 3/2/17, a conference call was held with KSU Representatives, The Georgia Secretary of State's Office, The Center for Election Systems, KSU Legal Affairs, and others. The call was to bring all parties up to speed and discuss next steps. Under the direction of the KSU CIO, at 7:00pm 03/03/17, UITS staff members [redacted] met with Merle King and seized the center for elections system [redacted] (KSU Tag 103019). A chain of evidence form was completed for the transaction and the server locked in UITS ISO Secure Storage (Pilcher 109A) which is behind auditable locks.

b6
b7C
b7E

The initial incident reporter [redacted] provided the following activity from the security researcher at 8:00pm 3/3/17

- Wednesday 02/22/17 - 6:00PM - 12:00AM EST - traffic originated from an Atlanta IP address and an IP address from Switzerland
- Friday 02/24/17 - 12:00PM - 8:00PM EST - traffic originated from an Atlanta IP address
- Tuesday 02/28/17 - 5:00PM - 12:00AM EST - traffic originated from an Atlanta IP address
- Wednesday 03/01/17 - 7:00PM - 10:00PM EST - traffic originated from an Atlanta IP address

UITS ISO Staff are currently working to use this additional data to correlate events to actors.

Logs to 2/16/2017

Some records in DB are still DLs using SSN.

- Aug 2016 - Bastille Security Researcher contacted KSU re: vuln. They addressed it.
- [redacted] are where IPs came from
  - content MGMT system
- No memory dump, machine has been powered down. no forensic image. No evidence of data being accessed.

Merle King - Director of Elections Center

b6
b7C
b7E

- one contained all 6.7 million
- others contained smaller subsets.
- [redacted] - no access to Center for Elections systems.

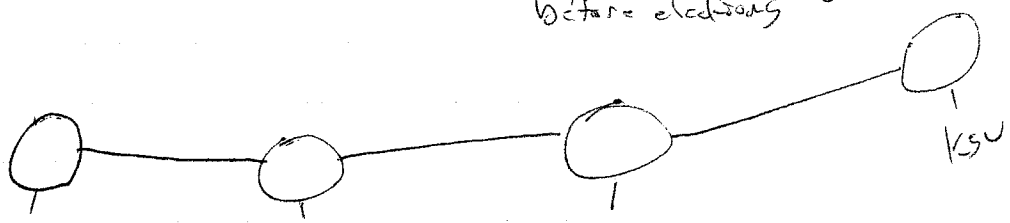
KSU Main

3/3/17

b7E

[redacted] goes back to Feb-17

1. ~~Atlanta~~ IP Addresses
2. 6.7 million records - may ~~not~~ add just before elections



Merle King - can answer questions about legitimate access.

Merle King - Dept. of CSIS @ Kennesaw

↓ 2002

Director of Center of Election Systems

Start of 2nd meeting

---

office / KSU vote

Washington Post Article - Merle King

Merle King told to block Bastille

b3
b7E

FD-302 (Rev. 5-8-10)

UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION

Date of entry 03/10/2017

On March 3, 2017, Special Agents (SAs) [redacted] and [redacted] and Computer Scientist [redacted] of the Federal Bureau of Investigation (FBI) participated in a meeting with Kennesaw State University (KSU) Information Technology (IT) personnel to include STEPHEN GAY and [redacted]. After being provided the identity of the interviewing agents and the nature of the interview, the following information was provided:

Flash Drive Summary:

[redacted] provided SA [redacted] with a flash drive containing data obtained during the course of KSU's incident response. Below is a description of the flash drive's content:

b6
b7C
b7E

[redacted]

CES Server:

The server was running [redacted]

[redacted]

UNCLASSIFIED//~~FOUO~~

Investigation on 03/03/2017 at Kennesaw, Georgia, United States (In Person)

File # [redacted] Date drafted 03/07/2017

by [redacted] SA [redacted]

b3
b7E
b6
b7C

[redacted] b7E

On or about August 2016, [redacted] a [redacted] at a company named BASTILLE, shared vulnerabilities that he discovered in the CES Server with MERLE KING, Executive Director at KSU's CES. It was believed [redacted] reached out to KING because he had been interviewed by media outlets, such as the Washington Post, and stated the election voter machines were unhackable. After [redacted] initial contact, KING asked KSU IT personnel to block email from bastille.net. b6 b7C

KSU maintains officially sanctioned twitter accounts for communication with the public. One of these accounts, @KSUVote, was used to share communications regarding the Center for Election Systems.

At the conclusion of the interview, [redacted] provided a hardcopy of an email in which [redacted] contacted KING on August 28, 2016.

Lastly, KSU IT personnel escorted the FBI to the location where the CES server was being securely stored. GAY signed a FD-941 "Consent to Search" form and relinquished custody of the CES server to the FBI. GAY was provided a copy FD-597 "Receipt for Property" form.

Copies of the FD-941 "Consent to Search" form, FD-597 "Receipt for Property" form, and a digital copy of [redacted] email along with the flash drive referenced above will been placed in the 1A section of the captioned case file.

Zimbra [redacted]

RE: [IMPORTANT] concerning the security of elections.kennesaw.edu

From : [redacted] Wed, Aug 31, 2016 02:46 PM

Subject : RE: [IMPORTANT] concerning the security of elections.kennesaw.edu

To : [redacted]

Cc [redacted], 'Michael Barnes [redacted]

[redacted] b7E

When is the earliest we can schedule more [redacted]

[redacted]

[redacted] b6 b7C b7E

Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: [redacted]
Fax: 678-915-4940

[redacted]

From: [redacted]
Sent: Wednesday, August 31, 2016 10:38
To: [redacted]
Cc: [redacted] Michael Barnes [redacted]
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Thanks [redacted] I see the list appears to be the same as from the [redacted] and I are working on a plan to [redacted]. Let me know if there is anything in [redacted] we should be concerned about that [redacted] may not fix. Thanks for all the help, we really appreciate your time. It has been immensely beneficial.

[redacted]
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P [redacted] F: 470-578-9012

On Aug 31, 2016, at 10:34 AM, [redacted] wrote:

[redacted]

The [redacted] completed last night and I will share the results as soon as my current meeting completes.

[redacted]
Information Security Office

[redacted]

University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel:
Fax: 678-915-4940

On Aug 31, 2016, at 10:00, > wrote:

Sounds good to us. Thanks

What is the status of the I couldn't find where it had been run and when I went to run the available options made it difficult to choose while not really understanding them.

KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: F: 470-578-9012

b6
b7C
b7E

On Wed, Aug 31, 2016 at 9:56 AM -0400, > wrote:

Hi

In addition to the we'd also like will focus more specifically on the will reach out to you

Regards,

Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone:
Fax: (470) 578-9051

----- Original Message -----
From:
To:
Cc: , "Michael Barnes
Sent: Tuesday, August 30, 2016 2:03:57 PM
Subject: RE: [IMPORTANT] concerning the security of elections.kennesaw.edu

Yes, this will be a

b7E

[redacted]

Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: [redacted]
Fax: 678-915-4940
[redacted]

From: [redacted]
Sent: Tuesday, August 30, 2016 12:21
To: [redacted]
Cc: [redacted] Michael Barnes [redacted] b6 b7C b7E
[redacted]
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu

Just to clarify, are the required credentials [redacted]

[redacted]

KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: [redacted] F: 470-578-9012

On Aug 30, 2016, at 11:59 AM, [redacted] > wrote:

[redacted]

Please log back in t[redacted] b7E
[redacted]

[redacted]

b7E

[redacted]

[redacted]

[redacted]

Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton Pl
Kennesaw, GA 30144
Tel: [redacted]
Fax: 678-915-4940
[redacted]

From: [redacted]
Sent: Monday, August 29, 2016 16:46
To: [redacted]
Cc: Michael Barnes [redacted]
[redacted]
Subject: Re: [IMPORTANT] concerning the security of elections.kennesaw.edu
[redacted]

b6
b7C
b7E

Thanks [redacted] I've logged into [redacted]
added. [redacted]

[redacted]

[redacted]

KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: [redacted] F: 470-578-9012

On Aug 29, 2016, at 4:22 PM, [redacted]
[redacted] wrote:

[redacted]

Hi

Thanks for reaching out. We can definitely assist in assessing the security and of your site. For starters, we can arrange for a to get some better insight.

to ensure that your site is following their best practices.

b6
b7C
b7E

Regards,

University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 026
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone:
Fax: (470) 578-9051

----- Original Message -----
From:
To:
Cc: "Michael Barnes"
"Merle S. King"
Sent: Monday, August 29, 2016 2:39:41 PM
Subject: Re: [IMPORTANT] concerning the security of

Good afternoon I wanted to reach out for some assistance with our website as suggested in Stephen's email below.

For some background information and I have taken responsibility for the website here at Center for Election Systems. before either of us were employed here and we have spent the last several years simply maintaining it in the order it had been working previously. Obviously this has become untenable in the current atmosphere, and and I must learn more to get the security of the website under control. In this regard we appreciate any help you can offer on security

best practices and specific security implementations that will allow us to secure the site.

This morning we implemented [redacted]

Please let [redacted] and I know if you have any insights that will help accomplish this goal, as well as get a local firewall set up to allow us to monitor access through logs. b6 b7C b7E

Thank you,

[redacted]
KSU Center for Election Systems
3205 Campus Loop Road
Kennesaw, GA 30144
P: [redacted] F: 470-578-9012

On Aug 29, 2016, at 11:31 AM, Stephen C. Gay < [redacted] wrote:

Michael,

Thanks for reaching out and we stand on ready to help. The source email domain, <http://bastille.net/>; bastille.net< <http://bastille.net/>; http://bastille.net/>;, has a valid domain registration through GoDaddy and located in Atlanta:

Registry Registrant ID:
Registrant Name: [redacted] b6 b7C
Registrant Organization: Bastille Networks
Registrant Street: 1000 Marietta St NW
Registrant Street: Suite 112
Registrant City: Atlanta
Registrant State/Province: GA
Registrant Postal Code: 30318
Registrant Country: US
Registrant Phone: +1.7328200096
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: <mailto:domains@bastillenetworks.com>
domains@bastillenetworks.com < <mailto:domains@bastillenetworks.com>
mailto:domains@bastillenetworks.com>

We don't put internal domain blocks in place unless we detect a spike in phishing or vulnerability scanning from that domain which, at this point, isn't the case for <http://bastille.net/>; bastille.net <
<http://bastille.net/>; http://bastille.net/>. It's very likely that the tester utilized Google searches on the [redacted] domain which included file extensions, along with HTML Headers which include the service versions.

Here the the Google search string which reveals the document he references
".pdf site:elections.kennesaw.edu"
Reporting precincts with cards -

[redacted] b7E

[redacted]

And here is the header response for [redacted]; [redacted] that gives away the use of [redacted] b7E

It is reasonable to assume that these types of unsolicited requests are going to increase leading up to the general election in November and we stand on ready to offer application security analysis and recommendations. In turn, I would highly recommend the use of an server based firewall/IDS to track this activity (specifically brute force attempts on the login page) and ensure that all access are logged.

I am cc'ing 2 members of my team, Mr. [redacted] and Mr [redacted], to advise on operating system/application vulnerabilities and provide advice on mitigating strategies. [redacted] will act as your point of contact and if I can assist in any way please let me know.

In service,

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050

[redacted]

----- Original Message -----
From: "Michael Barnes" <[redacted]
To: "Stephen C Gay" [redacted]
Cc: "Merle King" <[redacted] b6 b7C
Sent: Monday, August 29, 2016 9:24:30 AM
Subject: FW: [IMPORTANT] concerning the security of [redacted]

Stephen,

We received an unsolicited email over the weekend from a [redacted] The content of the email has engaged our staff and we are looking into these claims regarding the security of our website. Would you please add this individual and the organization he claims to be affiliated with to the list of IP addresses most recently black listed? Also, our IT staff, [redacted] and [redacted] will be reaching out to you and your staff to see what assistance your group can provide us in pinging our site to verify that we are addressing security issues within our site.

[redacted] b7E

Thank you in advance,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

From: Merle S. King [redacted]
Sent: Sunday, August 28, 2016 3:56 PM
To: Steven Dean <[redacted]
[redacted]
< <[redacted]
Cc: Michael Barnes [redacted]
Subject: Fwd: [IMPORTANT] concerning the security of
[redacted]

b6
b7C
b7E

Steven and Jason - Please review this email and advise. Sooner is better than later.

Thanks,

MSK

From: [redacted] <
[redacted]
To: "Merle King" <[redacted]
[redacted]
Cc: [redacted]
[redacted]
Sent: Sunday, August 28, 2016 3:47:50 PM
Subject: [IMPORTANT] concerning the security of
[redacted]

b6
b7C
b7E

Hello Merle,

My name is [redacted] and I'm a cybersecurity researcher who is a member of

Bastille Threat Research Team. We work to secure devices against new and

existing wireless threats: <https://www.bastille.net/>;
https://www.bastille.net/ < <https://www.bastille.net/>;
https://www.bastille.net/>;. This past Tuesday I
went

to Fulton County Government Center to speak with [redacted] about securing

voting machines against wireless threats. I was then directed to contact you

[redacted]

and the center. I'd like to collaborate with you on securing our state's election systems infrastructure against wireless attacks.

While attempting to get more background information on the center prior to contacting you, I discovered serious vulnerabilities affecting

[redacted]

The following google searches reveal documents that shouldn't be indexed and appear to be critical to the elections process. In addition, [redacted] b7E
install needs to be immediately [redacted]

[redacted]

I generally use this type of search to find documents on websites that lack search functionality. This search revealed a [redacted]

Assume any document that requires authorization has already been downloaded without authorization.

"site:elections.kennesaw.edu <[redacted]
[redacted] L&A"

The second search result appears to be for [redacted]

[redacted]

If you have any questions or concerns please contact me. I'm able to come to the center this Monday for a more thorough discussion.

Take care,

[redacted] b6 b7C

[redacted] b7E

--

Merle S. King

Executive Director

Center for Election Systems

Kennesaw State University

3205 Campus Loop Road

Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

b7E

[redacted]

3/3
DW/JZL
HR

→ [redacted] (SP?) HAS PWD

b6
b7C
b7E

EXPLOIT OCCURRED OUTSIDE OF CMS.

[redacted]

PROF [redacted] said researcher came from

[redacted]

TIMESTAMPS IN EST (UTC - 5)

[redacted]

9/-2014 [redacted] - Bastille.net showed vulnerabilities b6 b7C

to

Merle King was Information Systems Director 2002 → current CSIS. now director for center for electron system

Washington Post Article → ELECTION system is un hackable.

Merle King said to [redacted] b7E

[redacted]

DB3 - NOV 8 → present

2nd meeting

no contact of Bastille

3/3/17

USB

[redacted]

contact management

- may contain

[redacted]

[redacted]

b6
b7C
b7E

[redacted]

Apache2

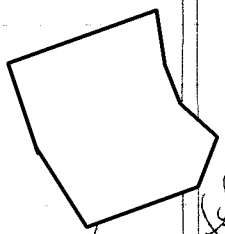
[redacted]

accessed by researcher

[redacted]

[redacted]

User Agent
↳ Mac
wget



↳ Bastille

[redacted]

allowed directory listings

Directory Browse

[redacted]

rule

[redacted]

Untitled

According to [redacted] this should access the [redacted]

b6
b7C
b7E

*U.S. GPO: 2004-305-792/81146

FD-597 (Rev 8-11-94)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) 3/3/17

item(s) listed below were:
- [x] Received From
- [ ] Returned To
- [ ] Released To
- [ ] Seized

(Name) Stephen C. Gay

(Street Address) CES, 1000 Chastain Road

(City) Kennesaw, GA

Description of Item(s):

1 Dell, PowerEdge R610, Service Tag: 96J2FQ1

DW

UNCLASSIFIED

Physical 1A/1C Cover Sheet for Serial Export

Created From:	[redacted]
Package:	1A8
Stored Location:	None
Summary:	(U) One Blue Verbatim Flash Drive
Acquired By:	SA [redacted]
Acquired On:	2017-03-03
Acquired From:	(U) CISO Stephen Gay Kennesaw State University
Attachment:	(U) One Blue Verbatim Flash Drive

b3
b6
b7C
b7E

[redacted]

b3
b7E

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: OTHER **Date:** 03/15/2017

Title: (U) Election-related files and usernames

Approved By: SSA [redacted]

Drafted By: SA [redacted]

b3
b6
b7C
b7E

Case ID #: [redacted] (U) UNSUB(S);
KENNESAW STATE UNIVERSITY - VICTIM;
COMPUTER INTRUSION - CRIMINAL MATTER;

Synopsis: (U) On March 06, 2017, Stephen Gay, CISO, Kennesaw State University, provided Special Agent [redacted] with documents associated with Election-related files and usernames for the Center for Elections website.

♦♦

March 3, 2017

Election-related files

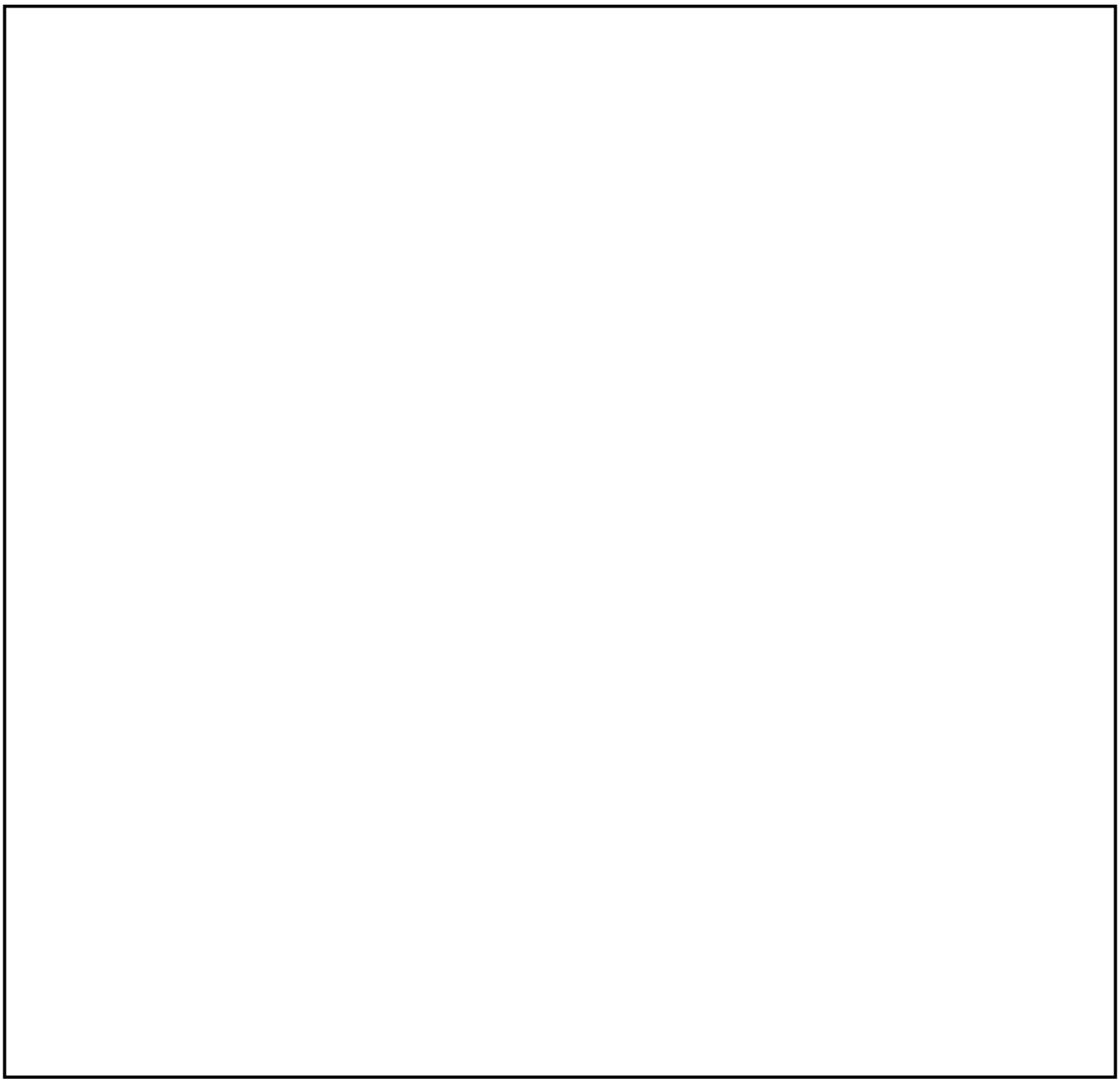
elections.kennesaw.edu

b7E

[redacted]

[redacted]

b7E



This concludes the types of files placed within the county folders for distribution to counties

b3
b7E

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 03/17/2017

date of birth (DOB) was interviewed at 30 Trammell Street SW, Marietta, Georgia. After being advised of the identity of the interviewing Agents and the nature of the interview, provided the following information:

During the interview, had his attorney, present. The interview was conducted at Marietta Office located at 30 Trammell Street SW, Marietta, Georgia.

On Wednesday, March 1, 2017, stated he received a text message from who is a security researcher and very active in the cyber security community about a possible cyber security issue at Kennesaw State University (KSU). subsequently spoke on the phone on the same day. informed that he recently had dinner with who is a at a company named Bastille. During this dinner, told about multiple vulnerabilities that he discovered with the KSU's Center for Elections System (CES) website (elections.kennesaw.edu). One of the vulnerabilities

b6
b7C
b7E

also informed that had previously discovered vulnerabilities in the CES website back in 2016. reported the vulnerabilities to KSU who supposedly fixed it. stated he has never met

After speaking with stated he got out his laptop and navigated to the website

After verifying the vulnerability, immediately contacted Stephen Gay who is the Chief Information Security Officer at KSU. recalled the notification was around 9:30 pm approximately.

Investigation on 03/10/2017 at Marietta, Georgia, United States (In Person)

File # Date drafted 03/14/2017

by SA

b3
b6
b7C
b7E

On Thursday, March 2, 2017, Gay contacted [redacted]. Gay wanted [redacted] to document the steps he took to verify the vulnerability. In addition, Gay wanted [redacted] to contact the security researchers and determine how they verified the vulnerability. [redacted] stated he collected the requested information and provided it to Gay via email on the same day. [redacted] stated the security researchers wanted to responsibly disclose the vulnerabilities so KSU could have time to mitigate the issues. Once mitigated, the security researchers wanted to discuss issuing a public notification so they could get credit for finding the vulnerabilities. The security researchers never demanded any money for finding the vulnerabilities.

On Friday, March 3, 2017, [redacted] communicated with [redacted] via text message after seeing news reports about a security incident at KSU's CES and the FBI being involved. [redacted] stated [redacted] was surprised to see the security incident in the news but thought the FBI being involved was a good thing.

b6
b7C

[redacted] stated he knew Merle King who is the Executive Director at KSU's CES. However, he has not spoken to King in approximately two years. King reached out to [redacted] about potentially conducting a penetration test against the CES website the last time the two spoke but the test never happened.

[redacted] provided [redacted] phone number [redacted] and a copy of his email exchanges with KSU. A copy of the emails will be maintained in the 1A section of the case file.

3/10/17

Wednesday

3/1/17 - [redacted] - arcsight so

- text

[redacted] had dinner w/ [redacted]

b6
b7C
b7E

reached out to Stephen Gay @ 9:30 pm on 3/1/17 app

Thursday

- Gay asked [redacted] to document his research ~~teacher~~ and the researchers activity

- no demand for money.

- responsible disclosure

doesn't know [redacted]

Friday

- spoke w/ [redacted] via text
- discuss writing news
-

b6
b7C
b7E

Conversation with [redacted]

Notebook: [redacted] notebook

Created: 3/1/2017 8:46 PM **Updated:** 3/1/2017 9:06 PM

Author: [redacted] **Location:** Cherokee County, Georgia, United...

[redacted]

- [redacted] - Bastille Networks - contact through [redacted]
  - Director of Marketing and Director of Research are in the loop

- talked to Merle [redacted] about 2 years
  - [redacted] wanted [redacted] about potential ~~[illegible]~~ penetrating. never happened

b6
b7C

- [redacted] said [redacted] found previously found vuln. in election server. & reported it to CISA.

Zimbra

[redacted]

Re: Vulnerability on the elections.kennesaw.edu website

From [redacted] Thu, Mar 02, 2017 08:00 PM
Subject : Re: Vulnerability on the elections.kennesaw.edu website
To [redacted], Stephen C. Gay [redacted]

Heard back from the researchers, here's what they shared with me:

[redacted]

b6
b7C
b7E

Thanks

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
[redacted]
Ph: [redacted]
Burruss Building, Room [redacted]

73656d7065722070617261747573

From: [redacted]
To: [redacted] "Stephen C. Gay" [redacted]
Sent: Thursday, March 2, 2017 2:56:45 PM
Subject: Re: Vulnerability on the elections.kennesaw.edu website

[redacted]

and Stephen,

I'm in the process of reaching out to the researcher(s) now, and will get back to you with any details they provide to me.

Please let me know if you need anything else.

Thanks

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
Ph:
Burruss Building, Room

b6
b7C
b7E

73656d70657220706172617261747573

From: "Stephen C. Gay"
To:
Cc:
Sent: Thursday, March 2, 2017 6:44:22 AM
Subject: Re: Vulnerability on the elections.kennesaw.edu website

Good morning. We are actively investigating this incident, specifically focusing on

[redacted] is coordinating the incident so if you could please send the information to him (cc'd on this email) I would appreciate it.

Thank you.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
[redacted]

b6
b7C
b7E

----- Original Message -----
From: [redacted]
To: "Stephen C Gay" [redacted]
Sent: Wednesday, March 1, 2017 9:55:27 PM
Subject: Vulnerability on the elections.kennesaw.edu website

Stephen,

Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a [redacted] vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for [redacted]

My friend shared with me that the [redacted]

I was able to verify the presence of the vulnerability myself, and was able to [redacted]

I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to [redacted]

releasing to the public, I'm hopeful that my sense is correct.

If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

Thanks

[redacted] b6 b7C

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

[redacted]

Ph[redacted]
Burruss Building, Room [redacted]

73656d7065722070617261747573

[redacted] b7E

Zimbra [redacted]

Re: Vulnerability on the elections.kennesaw.edu website

From : [redacted] Thu, Mar 02, 2017 02:56 PM

Subject : Re: Vulnerability on the elections.kennesaw.edu website

To [redacted], Stephen C. Gay [redacted]

[redacted]and Stephen,

I'm in the process of reaching out to the researcher(s) now, and will get back to you with any details they provide to me.

[redacted] b6 b7C b7E

Please let me know if you need anything else.

Thanks

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
[redacted]
Ph: [redacted]
Burruss Building, Room [redacted]

73656d70657220706172617261747573

From: "Stephen C. Gay" [redacted]
To: [redacted]
Cc: [redacted]

[redacted]

Sent: Thursday, March 2, 2017 6:44:22 AM
Subject: Re: Vulnerability on the elections.kennesaw.edu website

[redacted]

Good morning. We are actively investigating this incident, specifically focusing on the scope of data disclosure. With that in mind, we are seeking your assistance in determining when and from where the security researcher(s) accessed the elections.kennesaw.edu data. Likewise, can you please share when you accessed [redacted]

[redacted] is coordinating the incident so if you could please send the information to him (cc'd on this email) I would appreciate it.

Thank you.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
[redacted]

b6
b7C
b7E

----- Original Message -----
From: [redacted]
To: "Stephen C Gay" <sgay@kennesaw.edu>
Sent: Wednesday, March 1, 2017 9:55:27 PM
Subject: Vulnerability on the elections.kennesaw.edu website

Stephen,

Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a [redacted] vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows [redacted]

My friend shared with me that the [redacted]

I was able to verify the presence of the vulnerability myself, and was able to [redacted]

[redacted]

I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

Thanks

b6
b7C
b7E

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

[redacted]

Ph[redacted]
Burruss Building, Room [redacted]

73656d70657220706172617261747573

[redacted]

Zimbra

Re: Vulnerability on the elections.kennesaw.edu website

From : Stephen C. Gay Thu, Mar 02, 2017 06:44 AM
Subject : Re: Vulnerability on the elections.kennesaw.edu website
To
Cc :

Good morning. We are actively investigating this incident, specifically focusing on

is coordinating the incident so if you could please send the information to him (cc'd on this email) I would appreciate it.

b6
b7C
b7E

Thank you.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050

----- Original Message -----
From:
To: "Stephen C Gay"
Sent: Wednesday, March 1, 2017 9:55:27 PM
Subject: Vulnerability on the elections.kennesaw.edu website

Stephen,

Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a

vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for [redacted]

My friend shared with me that the [redacted]

I was able to verify the presence of the vulnerability myself, and was able to [redacted]

I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

Thanks

b6
b7C
b7E

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

[redacted]

Ph: [redacted]
Burruss Building, Room [redacted]

[redacted]

73656d7065722070617261747573

b7E

Zimbra [redacted]

Re: Need to speak with you in-person

From : [redacted] Wed, Mar 01, 2017 09:56 PM

Subject : Re: Need to speak with you in-person

To : Stephen C. Gay [redacted]

I think our emails passed each other, you should have the details now.

Thanks

[redacted]

b6
b7C
b7E

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

[redacted]

Ph: [redacted]
Burruss Building, Room [redacted]

73656d70657220706172617261747573

From: "Stephen C. Gay" [redacted]
To: [redacted]
Sent: Wednesday, March 1, 2017 9:47:49 PM
Subject: Re: Need to speak with you in-person

[redacted]

I've got the team on standby and we are awaiting the information on the conduit for the alleged breach. Please send to me as soon as possible.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031

[redacted]

1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
[redacted]

----- Original Message -----
From: [redacted]
To: "Stephen C Gay" [redacted]
Sent: Wednesday, March 1, 2017 9:27:33 PM
Subject: Re: Need to speak with you in-person

This needs to happen immediately. It's that serious.

Can you talk now, by phone?

Thanks

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
[redacted]
Ph: [redacted]
Burruss Building, Room [redacted]

b6
b7C
b7E

73656d70657220706172617261747573

From: "Stephen C. Gay" [redacted]
To: [redacted]
Sent: Wednesday, March 1, 2017 9:26:08 PM
Subject: Re: Need to speak with you in-person

[redacted]

I'm closing on a house tomorrow and will be out of the office until Monday, then afterwards to Friday. Can we meet on Monday, or can I call you on Friday?

Stephen

Sent from Nine

[redacted]

From: [redacted]
Sent: Mar 1, 2017 9:23 PM
To: Stephen C. Gay
Subject: Need to speak with you in-person

Stephen,

I need to speak with you in-person regarding a very sensitive matter. Due to the importance of the issue, this conversation needs to happen immediately.

Please let me know when make time to meet with me.

Thanks

b6
b7C
b7E

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

[redacted]

Ph: [redacted]
Burruss Building, Room [redacted]

73656d7065722070617261747573

[redacted]

Zimbra

Vulnerability on the elections.kennesaw.edu website

From [redacted] Wed, Mar 01, 2017 09:55 PM

Subject : Vulnerability on the elections.kennesaw.edu website

To : Stephen C. Gay [redacted]

Stephen,

Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a [redacted] vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for [redacted]

My friend shared with me that the [redacted]

I was able to verify the presence of the vulnerability myself, and was able to [redacted]

b6
b7C
b7E

I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

Thanks

[redacted]

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

[redacted]

Ph: [redacted]
Burruss Building, Room [redacted]

b6
b7C
b7E

73656d706572207061726174573

[redacted]

Zimbra [redacted]

Re: Need to speak with you in-person

From : Stephen C. Gay [redacted] Wed, Mar 01, 2017 09:47 PM
Subject : Re: Need to speak with you in-person
To : [redacted]

[redacted]

I've got the team on standby and we are awaiting the information on the conduit for the alleged breach. Please send to me as soon as possible.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
[redacted]

b6
b7C
b7E

----- Original Message -----
From: [redacted]
To: "Stephen C Gay" [redacted]
Sent: Wednesday, March 1, 2017 9:27:33 PM
Subject: Re: Need to speak with you in-person

This needs to happen immediately. It's that serious.

Can you talk now, by phone?

Thanks

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405

[redacted]

Kennesaw, GA 30144-5591
[redacted]
Ph: [redacted]
Burruss Building, Room [redacted]

73656d7065722070617261747573

b6
b7C
b7E

From: "Stephen C. Gay" [redacted]
To: [redacted]
Sent: Wednesday, March 1, 2017 9:26:08 PM
Subject: Re: Need to speak with you in-person

[redacted]

I'm closing on a house tomorrow and will be out of the office until Monday, then afterwards to Friday. Can we meet on Monday, or can I call you on Friday?

Stephen

Sent from Nine

From: [redacted]
Sent: Mar 1, 2017 9:23 PM
To: Stephen C. Gay
Subject: Need to speak with you in-person

Stephen,

I need to speak with you in-person regarding a very sensitive matter. Due to the importance of the issue, this conversation needs to happen immediately.

b6
b7C
b7E

Please let me know when make time to meet with me.

Thanks

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
[redacted]
[redacted]

[redacted]

Ph: [redacted]
Burruss Building, Room [redacted]

73656d70657220706172617261747573

b6
b7C
b7E

Zimbra [redacted]

Re: Need to speak with you in-person

From : Stephen C. Gay [redacted] Wed, Mar 01, 2017 09:28 PM
Subject : Re: Need to speak with you in-person
To : [redacted]

Sure, give me a call on my cell [redacted]

Stephen

Sent from Nine

From: [redacted]
Sent: Mar 1, 2017 9:27 PM
To: Stephen C. Gay
Subject: Re: Need to speak with you in-person

b6
b7C
b7E

This needs to happen immediately. It's that serious.

Can you talk now, by phone?

Thanks

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

[redacted]

Ph: [redacted]
Burruss Building, Room [redacted]

73656d70657220706172617261747573

From: "Stephen C. Gay" [redacted]
To: [redacted]

[redacted]

Sent: Wednesday, March 1, 2017 9:26:08 PM
Subject: Re: Need to speak with you in-person

[redacted]

I'm closing on a house tomorrow and will be out of the office until Monday, then afterwards to Friday. Can we meet on Monday, or can I call you on Friday?

Stephen

Sent from Nine

From: [redacted]
Sent: Mar 1, 2017 9:23 PM
To: Stephen C. Gay
Subject: Need to speak with you in-person

b6
b7C
b7E

Stephen,

I need to speak with you in-person regarding a very sensitive matter. Due to the importance of the issue, this conversation needs to happen immediately.

Please let me know when make time to meet with me.

Thanks

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

[redacted]

Ph: [redacted]
Burruss Building, Room [redacted]

73656d7065722070617261747573

[redacted]

Zimbra

[redacted]

Re: Need to speak with you in-person

From [redacted] Wed, Mar 01, 2017 09:27 PM
Subject : Re: Need to speak with you in-person
To : Stephen C. Gay [redacted]

This needs to happen immediately. It's that serious.

Can you talk now, by phone?

Thanks

[redacted]

b6
b7C
b7E

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
[redacted]
Ph: [redacted]
Burruss Building, Room [redacted]

73656d70657220706172617261747573

From: "Stephen C. Gay" [redacted]
To: [redacted]
Sent: Wednesday, March 1, 2017 9:26:08 PM
Subject: Re: Need to speak with you in-person

[redacted]

I'm closing on a house tomorrow and will be out of the office until Monday, then afterwards to Friday. Can we meet on Monday, or can I call you on Friday?

Stephen

Sent from Nine

[redacted]

From: [redacted]
Sent: Mar 1, 2017 9:23 PM
To: Stephen C. Gay
Subject: Need to speak with you in-person

Stephen,

I need to speak with you in-person regarding a very sensitive matter. Due to the importance of the issue, this conversation needs to happen immediately.

Please let me know when make time to meet with me.

Thanks

b6
b7C
b7E

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

[redacted]

Ph: [redacted]
Burruss Building, Room [redacted]

73656d706572207061726174573

[redacted]

Zimbra [redacted]

Re: Need to speak with you in-person

From : Stephen C. Gay [redacted] Wed, Mar 01, 2017 09:26 PM
Subject : Re: Need to speak with you in-person
To : [redacted]

[redacted]

I'm closing on a house tomorrow and will be out of the office until Monday, then afterwards to Friday. Can we meet on Monday, or can I call you on Friday?

Stephen

Sent from Nine

b6
b7C
b7E

From: [redacted]
Sent: Mar 1, 2017 9:23 PM
To: Stephen C. Gay
Subject: Need to speak with you in-person

Stephen,

I need to speak with you in-person regarding a very sensitive matter. Due to the importance of the issue, this conversation needs to happen immediately.

Please let me know when make time to meet with me.

Thanks

[redacted]

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

[redacted]

Ph: [redacted]
Burruss Building, Room [redacted]

[redacted]

73656d7065722070617261747573

Zimbra [redacted]

Need to speak with you in-person

From : [redacted] Wed, Mar 01, 2017 09:23 PM

Subject : Need to speak with you in-person

To : Stephen C. Gay [redacted]

Stephen,

I need to speak with you in-person regarding a very sensitive matter. Due to the importance of the issue, this conversation needs to happen immediately.

Please let me know when make time to meet with me.

Thanks

[redacted]

b6
b7C
b7E

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591
[redacted]
Ph: [redacted]
Burruss Building, Room [redacted]

73656d706572207061726174573

[redacted] Num Agt. [redacted]

C [redacted]

offa [redacted]

[redacted]

[redacted]

b3
b7E

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 03/27/2017

[redacted] date of birth (DOB) [redacted] was interviewed at his residence located at [redacted] Atlanta, Georgia. After being advised of the identity of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

[redacted] Web Sight (website.io). In addition, [redacted] stated he and [redacted] who is a [redacted] at the company Bastille have been working together on research where they have identified several security vulnerabilities in a particular type of software. In following the responsible disclosure protocol, [redacted] and [redacted] notified the software company of the vulnerabilities. They are working with the company to resolve the vulnerabilities and potentially present their research at the Defcon Cyber Security Conference in Las Vegas, Nevada this year.

On Wednesday, February 22, 2017, [redacted] were at [redacted] house working on the research mentioned above. During one of their conversations, [redacted] stated he wished he could have published his research on the Kennesaw State University's (KSU) Center of Elections (CES) Website. [redacted] had found several security vulnerabilities with the website. [redacted] discussed his findings with his supervisors at Bastille. [redacted] supervisors stated there was no way in hell they wanted to report on anything related to elections. However, [redacted] still notified KSU CES directly of his findings who supposedly resolved the issues.

b6
b7C
b7E

[redacted] stated he and [redacted] decided to see if KSU actually resolved the issues. In conducting some basic searches, they immediately discovered [redacted] vulnerabilities for the [redacted] on the KSU CES website that allowed [redacted]

While conducting this research at [redacted] house, [redacted] was using the [redacted] did not know if [redacted] was using a [redacted] or not. In addition,

Investigation on 03/16/2017 at Atlanta, Georgia, United States (In Person)

File # [redacted] Date drafted 03/17/2017

by SA [redacted]

b3
b6
b7C
b7E

used the following three programs to test the website:

stated he was very concerned about the security vulnerabilities in the KSU CES website. After about a week of thinking about it, stated he contacted and told him that he was going to report their findings to who is a professor at KSU. stated he had previously met at one of the Atlanta B-Sides conferences in Atlanta, Georgia.

b3
b6
b7C
b7E

On March 01, 2017, notified stated he accessed the KSU CES website again while discussing the vulnerabilities with During this time, accessed the website from his residence using just the IP address assigned by his Internet Service Provider (ISP) Google Fiber and not the VPN service previously used. stated he believes the IP address assigned to him during this time was also provided his IPv6 IP address assigned by Google Fiber.

stated that he only downloaded one database file from the KSU CES website as a proof of concept during all of his research but had already deleted the file from his computer.

[redacted]

3/16/17

2/22/2017

Wednesday [redacted] reached to

October - published research

b6
b7C
b7E

[redacted]

- raised concerns to ~~[redacted]~~ sops but ~~[redacted]~~ would ~~[redacted]~~ not report.
- notified FSU election officially

[redacted]

2/22/17

- from [redacted] house - 2/24/17, 2/28/17

-

[redacted]

[redacted]

Atlanta b-sides / met [redacted]

Interview of [redacted]

- Doing research with [redacted]
- Met on Wednesday unknown date
- [redacted] mentioned in passing
- [redacted] reached out to KSU after ~~today~~ selection committee
- KSU patched [redacted]
- [redacted] initially
- Followed with Professor [redacted] within 2-3 weeks
- Provided list of times accessed to [redacted]
- Believes IP of [redacted] Place is Comcast
- Google Fiber IP is his home IP [redacted]
- Downloaded one ~~DB~~ file just since deleted

b6
b7C
b7E

FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 03/27/2017

On March 17, 2017, Special Agent (SA) [redacted] returned the Center of Elections (CES) server collected on March 03, 2017 to Stephen Gay who is the Chief Information Security Officer at Kennesaw State University. In addition, SA [redacted] provided Gay with a CD containing a spreadsheet with [redacted] logs. b3 b6 b7C b7E

Copies of the FD-597 Receipt of Property and the spreadsheet provided to Gay will be maintained in the 1A section of the case file.

Investigation on 03/17 [redacted] at Kennesaw, Georgia, United States (In Person)

File # [redacted] Date drafted 03/27/2017

by SA [redacted] b3 b6 b7C b7E

*U.S. GPO: 2004-307-714/90013

FD-597 (Rev 8-11-94)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) 3/17/17

item(s) listed below were:
- ☐ Received From
- ☑ Returned To
- ☐ Released To
- ☐ Seized

(Name) Stephen C. Gay

(Street Address) CES, 1000 Chastain Road

(City) Kennesaw, GA

Description of Item(s):

1 Dell, PowerEdge R610, Service Tag: 96J2FQ1

Received By: _____ (Signature)

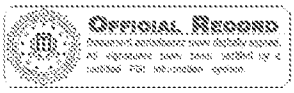
Received From: [redacted]

b6
b7C
DW

[redacted]

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED



FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: OTHER **Date:** 03/30/2017

Title: (U) [redacted] Preservation Letter

Approved By: SSA [redacted]

Drafted By: SA [redacted]

Case ID #: [redacted] (U) UNSUB(S);
KENNESAW STATE UNIVERSITY - VICTIM;
COMPUTER INTRUSION - CRIMINAL MATTER;

b3
b6
b7C
b7E

Synopsis: (U) [redacted] Preservation Letter for [redacted]

♦♦

UNCLASSIFIED

U.S. Department of Justice

Federal Bureau of Investigation

2635 Century Parkway NE
Atlanta, Georgia 30345
March 29, 2017

[redacted]

Dear Custodian of Records:

This letter will serve as a formal request for the preservation of records and other evidence pursuant to Title 18, use, Section 2703(f) pending further legal process.

You are hereby requested to preserve, for a period of 90 days, the records described below currently in media, in a form that includes the complete record. You also are requested not to disclose the existence other than is necessary to comply with this request. You are further requested not to terminate the account listed in this request if such termination is solely due to the receipt of this request. Further, allowing this account to remain active may assist Law Enforcement efforts.

This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request.

This preservation request applies to the following records and evidence:

[redacted]

b6
b7C
b7E

Please direct any questions you may have about this order to **Special Agent** [redacted]

b6
b7C
b7E

Sincerely,

[redacted]
Special [redacted] in Charge

[redacted]
Supervisory Special Agent

FD-448
Revised
10-27-2004

FEDERAL BUREAU OF INVESTIGATION

FACSIMILE COVER SHEET

PRECEDENCE

○ Immediate ○ Priority ◉ Routine

CLASSIFICATION

○ Top Secret ○ Secret ◉ Confidential ○ Sensitive ○ Unclassified

TO

Name of Office: [redacted]

Facsimile Number: [redacted]

Date: **03/29/2017**

Attn: **Custodian of Records**

Room:

Telephone Number: [redacted]

FROM

Name of Office: **FBI Atlanta**

Number of Pages: (including cover) **3**

Originator's Name: **SA** [redacted]

Originator's Telephone Number: [redacted]

Originator's Facsimile Number: **404-679-1417**

Approved:

DETAILS

Subject:
Preservation Letter

Special Handling Instructions:

Brief Description of Communication Faxed:

WARNING

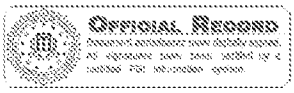
Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or local FBI Office immediately to arrange for proper disposition.

b6
b7C
b7E

[redacted]

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED



FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: OTHER **Date:** 03/30/2017

Title: (U) [redacted] Preservation Letter

b6
b7C
b7E

Approved By: SSA [redacted]

Drafted By: SA [redacted]

Case ID #: [redacted] (U) UNSUB(S);
KENNESAW STATE UNIVERSITY - VICTIM;
COMPUTER INTRUSION - CRIMINAL MATTER;

Synopsis: (U) [redacted] Preservation Letter for [redacted] The preservation letter was assigned [redacted]

♦♦

UNCLASSIFIED

U.S. Department of Justice

Federal Bureau of Investigation

2635 Century Parkway NE
Atlanta, Georgia 30345
March 29, 2017

[redacted]

b6
b7C
b7E

Dear Custodian of Records:

This letter will serve as a formal request for the preservation of records and other evidence pursuant to Title 18, use, Section 2703(f) pending further legal process.

You are hereby requested to preserve, for a period of 90 days, the records described below currently in media, in a form that includes the complete record. You also are requested not to disclose the existence other than is necessary to comply with this request. You are further requested not to terminate the account listed in this request if such termination is solely due to the receipt of this request. Further, allowing this account to remain active may assist Law Enforcement efforts.

This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request.

This preservation request applies to the following records and evidence:

[redacted]

b6
b7C
b7E

Please direct any questions you may have about this order to **Special Agent** [redacted]

Sincerely,

[redacted]

Special [redacted]

Supervisory Special Agent

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: OTHER **Date:** 03/30/2017

Title: (U) [redacted] Preservation Letter

b6
b7C
b7E

Approved By: SSA [redacted]

Drafted By: SA [redacted]

Case ID #: 288A-AT-2141248 (U) UNSUB(S);
KENNESAW STATE UNIVERSITY - VICTIM;
COMPUTER INTRUSION - CRIMINAL MATTER;

Synopsis: (U) [redacted] Preservation Letter for [redacted]

♦♦

UNCLASSIFIED

U.S. Department of Justice

Federal Bureau of Investigation

2635 Century Parkway NE
Atlanta, Georgia 30345
March 29, 2017

b6
b7C
b7E

Dear Custodian of Records:

This letter will serve as a formal request for the preservation of records and other evidence pursuant to Title 18, use, Section 2703(f) pending further legal process.

You are hereby requested to preserve, for a period of 90 days, the records described below currently in media, in a form that includes the complete record. You also are requested not to disclose the existence other than is necessary to comply with this request. You are further requested not to terminate the account listed in this request if such termination is solely due to the receipt of this request. Further, allowing this account to remain active may assist Law Enforcement efforts.

This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request.

This preservation request applies to the following records and evidence:

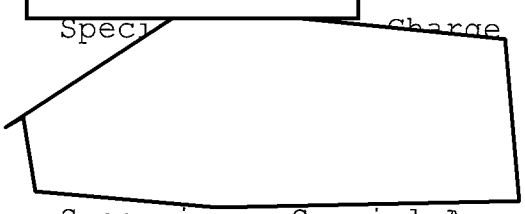
Please direct any questions you may have about this order to **Special Agent** [redacted]

b6
b7C
b7E

Sincerely,

[redacted]

Special Agent in Charge



Supervisory Special Agent

[redacted]

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: UNET-EMAIL **Date:** 04/04/2017

Title: (U) Email from Stephen Gay, KSU

Approved By: SSA [redacted]

Drafted By: SA [redacted]

Case ID #: [redacted] (U) UNSUB(S);
KENNESAW STATE UNIVERSITY - VICTIM;
COMPUTER INTRUSION - CRIMINAL MATTER;

b3
b6
b7C
b7E

Synopsis: (U) Email from Stephen Gay, CISO, KSU, dated March 21, 2017. The email was related to [redacted]

Enclosure(s): Enclosed are the following items:
1. (U) Excel Spreadsheet containing [redacted]

♦♦

From: Stephen C. Gay
Sent: Tuesday, March 21, 2017 4:15 PM
To: AT) (FBI)
Subject:
Attachments:

Agent

b6
b7C
b7E

Following up on the CD you provided Friday, a member of the team in a new spreadsheet (attached) which denotes any additional information we may have on I'm passing along in hopes that it will ultimately help you in determining whether there are

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director Information Security Office University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050

FEDERAL BUREAU OF INVESTIGATION

Date of entry 04/12/2017

On March 30, 2017, representatives from the Atlanta Division of the Federal Bureau of Investigation (FBI) as well as the United States Attorney's Office, Northern District of Georgia (USAO-NDGA), met with executives of Kennesaw State University (KSU) in the KSU Presidential Boardroom. The individuals in attendance included:

Federal Bureau of Investigation

[redacted] Supervisory Special Agent
[redacted] Special Agent
[redacted] Special Agent

b3
b6
b7C
b7E

United States Attorney's Office

[redacted] Deputy Chief, Criminal Division
Assistant United States Attorney

Kennesaw State University

Samuel S. Olens, President
Lectra Lawhorne, Chief Information Officer/VPIT
Stephen C. Gay, Chief Information Security Officer
Merle S. King, Executive Director, Center for Election Systems

The purpose of the meeting was for the FBI and USAO to share information with KSU executives related to the alleged breach of a server associated with elections.kennesaw.edu.

In summary, SSA [redacted] provided KSU executives with a high-level overview of investigative findings related to the case. SSA [redacted] advised during the course of the investigation, the FBI [redacted] provided by KSU, [redacted] and conducted interviews. During the investigation, the FBI identified a security researcher who found at least

one vulnerability associated with elections.kennesaw.edu. The FBI provided the investigative findings to the NDGA USAO's office who determined no federal statute had been violated by the security researcher.

b3
b6
b7C
b7E

SSA [redacted] and AUSA [redacted] advised KSU executives due to the limited [redacted] provided by KSU, the investigation did not encompass the full scope of time the server may have been compromised.

President Olens advised KSU was working with a third-party firm as well as Georgia Tech to review the security of their servers. He also praised the FBI and USAO's prompt investigation.

FD-302 (Rev. 5-8-10)

b3 b6 b7C b7E

FEDERAL BUREAU OF INVESTIGATION

Date of entry 10/23/2017

Special Agent (SA) [redacted] and SA [redacted] conducted a [redacted] into an alleged compromise of the Kennesaw Stated University (KSU) Center for Election Systems (CES) website (elections.kennesaw.edu). The [redacted]. No investigative activity has been conducted on the case since August 18, 2017.

SA [redacted] requests the evidence item 1B-1 (one (1) Seagate 2 TB SATA HDD, S/N 5XW2AP34, containing image of Dell PowerEdge R610 Server, S/N 96J2FQ1) be transferred to case file [redacted]. Once completed, the case file will be closed.

b7A

Investigation on 10/20/2017 at Atlanta, Georgia, United States (, Other (Transfer of Evidence))

File # [redacted] Date drafted 10/20/2017

by SA [redacted]

b3 b6 b7C b7E